

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

LINDA CRAWFORD and MICHAEL
PRICE, on behalf of themselves and all
others similarly situated,

Plaintiffs,

v.

MCG HEALTH, LLC,

Defendant.

Case No.

**COMPLAINT - CLASS ACTION
DEMAND FOR JURY TRIAL**

Plaintiffs, Linda Crawford (“Ms. Crawford”) and Michael Price (“Mr. Price”), through their attorneys, bring this Class Action Complaint against the Defendant, MCG Health, LLC (“MCG” or “Defendant”), alleging as follows:

I. INTRODUCTION

1. In December 2021, MCG—a technology company that collects and stores patient data from hospitals across the country—discovered that cybercriminals had stolen the highly sensitive personal and medical information belonging to over 1.1 million patients (“Data Breach”), and then misrepresented how the Data Breach happened when it notified patients about the breach *six* months later.

2. On information and belief, cybercriminals could bypass and breach MCG’s security systems because MCG does not adhere to industry-standard cybersecurity policies, state and federal law, or its own data security policies, which promise to use “reasonable efforts” to protect sensitive information. *See* MCG’s Privacy Policy at <https://www.mcg.com/privacy-policy/> (last visited June 22, 2022). MCG failed to do so even though it recognizes that companies must be “more diligent than ever” in implementing cybersecurity policies given “the value of the information” they collect. *See* MCG’s article: *Cybercrime Prevention: Protect Your Passwords* <https://www.mcg.com/blog/2017/10/30/cybercrime-password-protection/> (last visited June 22, 2022).

3. As a result, MCG left millions of patients’ highly sensitive personally identifiable information (“PII”) and protected health information (“PHI”) an ungarded target for theft and misuse.¹

4. Worse yet, MCG’s late-arriving breach notice to patients (“Breach Notice”) misrepresents when and how the breach happened. The Breach Notice claims that MCG learned about the breach in March 2022, but MCG’s hospital customers disclosed that MCG knew about the breach as early as December 2021. In fact, UNC Lenoir Health Care disclosed that cybercriminals had stolen patient information from MCG and posted it for sale on the dark web:

¹ Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d et seq., and its implementing regulations (“HIPAA”), “protected health information” is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 Protected health information. A “covered entity” is further defined to include health care providers and their “business associates,” such as MCG.

In December of 2021 and again in January of 2022, MCG was contacted by an unknown third-party who claimed to have improperly obtained patient data from MCG. This third-party made a demand for money in exchange for the return of the patient data to MCG. MCG opened an investigation and contacted the FBI. MCG made Lenoir aware of this incident on April 24, 2022. MCG's forensic investigators confirmed that records for ten (10) patients were listed by this third party for sale on the dark web. These records are believed to have come from MCG. Lenoir patient records were not found on the dark web, but MCG has determined that the unauthorized third-party may be in possession of Lenoir information which could include: patient name, Social Security number, medical codes, street address, telephone number, email address, date of birth and gender.

See UNC Lenoir Health Care's breach notice,

https://www.unclenoir.org/app/files/public/eee43670-ad21-4614-b099-89661edd7166/pdf-lenoir-LEN%20PR%201017_Substitute%20Notice_6.13.2022%20FINAL.pdf (last visited June 23, 2022).

5. But MCG's Breach Notice did not disclose this information. Instead, MCG obfuscated and hid the nature of the breach from its victims:

MCG determined on March 25, 2022 that an unauthorized party previously obtained certain personal information about affected individuals that matched data stored on MCG's systems. The affected data included some or all of the following data elements: names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth and gender.

Upon learning of this issue, MCG took steps to understand its nature and scope. A leading forensic investigation firm was retained to assist in the investigation. Additionally, MCG is coordinating with law enforcement. MCG has deployed additional monitoring tools and will continue to enhance the security of its systems.

A true and accurate copy of MCG's Breach Notice to patients is attached hereto as **Exhibit A**.

6. Indeed, the Breach Notice does not disclose who "previously obtained" patients' highly sensitive information, when they stole it, how they did so undetected, whether they posted information on the dark web, whether they ransomed MCG, or why it took MCG six months to send a bare bones notice about the breach.

7. Following the breach, MCG claims that it "deployed additional monitoring tools and will continue to enhance the security of our systems"—"monitoring tools" and "enhancements" that should have been in place *before* the Data Breach.

1 the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100
 2 members in the proposed class, and at least one member of the class is a citizen of a state
 3 different from Defendant.

4 15. This Court has personal jurisdiction over Defendant because MCG is
 5 headquartered in this District and MCG conducts substantial business in this District.

6 16. Venue is proper in this District because MCG is headquartered in this District
 7 and a substantial part of the events or omissions giving rise to Ms. Crawford's claims occurred
 8 in this District.

9 **IV. BACKGROUND FACTS**

10 **A. MCG**

11 17. MCG advertises that it provides "Cutting Edge Software and Unbiased Clinical
 12 Guidelines" to healthcare organizations.

13 18. In so doing, MCG claims that it uses "[n]ew technology developments, like
 14 artificial intelligence," boasting about its technical solutions.

15 19. As part of its business, MCG collects patient PII and PHI from its customers,
 16 including hospitals across the country, thus accruing vast amounts of private information.

17 20. In collecting this information, MCG understands it has a duty to protect it using
 18 adequate data security. Specifically, MCG's privacy policy promises that MCG will use
 19 "reasonable means" to protect patient data using a "variety of security technologies and
 20 procedures to help protect information from unauthorized access, use, or disclosure." *See*
 21 MCG's Privacy Policy at <https://www.mcg.com/privacy-policy/> (last visited June 22, 2022).
 22
 23
 24
 25
 26
 27

21. Further, MCG knows that cybercriminals target companies like MCG because they know how valuable a person's PII and PHI are to hackers. Indeed, MCG published an article that advises companies to be "more diligent than ever" given "the value of the information" that they protect:

The security landscape of technology has really changed, especially in the last few years. The rise of cloud computing (and distributed computing) has given hackers much more powerful tools and we've seen extremely high-profile cybercrime activity exhibiting much greater complexity and sophistication. We now live in a world where the best hackers (and hacker groups) lease out their services to the highest bidder, and it's time to be more diligent than ever.

One of the largest breaches of recent note is the one involving [Equifax](#), a consumer credit reporting agency, and if you're reading this then there is an extremely high chance that you have been affected. The Equifax breach is so important because of the value of the information; hackers stole enough information that they now have actionable data which would allow them to fill out phony credit applications, or even help them in accessing your bank accounts or personal information from other services.

See MCG's article: *Cybercrime Prevention: Protect Your Passwords*

<https://www.mcg.com/blog/2017/10/30/cybercrime-password-protection/> (last visited June 22, 2022).

22. But despite recognizing its duty to protect the vast amounts of PII and PHI it collects, on information and belief, MCG does not adhere to industry-standard data security policies, its own policies, or state and federal law. Indeed, on information and belief, MCG has not implemented reasonable cybersecurity safeguards to protect patient PII and PHI, leaving it an unguarded target for cybercriminals to steal and misuse.

B. MCG Fails to Safeguard Patient PII and PHI and Misrepresents How the Breach Happened

23. Plaintiffs are former patients at customers of MCG.

24. As part of MCG's services to its customers, MCG collects PII and PHI relating to patients and/or employees, including Plaintiffs.

25. In so doing, MCG collects and maintains the patient and/or employee PII and PHI in its computer systems.

26. In collecting and maintaining the PII and PHI, MCG agreed it would safeguard the data according to its internal policies and state and federal law. Further, MCG has a duty to notify patients about data breaches soon after they occur, giving them an opportunity to safeguard themselves against identity theft.

27. MCG failed in those duties.

28. MCG *claims* it discovered the Data Breach in March 2022, finding that cybercriminals had "previously" breached its systems and stole the PII and PHI belonging to over 1.1 million patients. That data included patients' "names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and genders."

29. On discovering the breach, MCG also claims it started an internal investigation to "understand its nature and scope."

30. That investigation inexplicably dragged on for months and culminated in a Breach Notice that yielded little about the breach's "nature and scope."

31. Indeed, despite disclosing that cybercriminals had "previously obtained" patients' PII and PHI, MCG was unwilling or unable to disclose *when* they did so. What's more, MCG did not detail *who* stole the data, *how* they did it undetected, *what* they did with it after they stole it, *whether* MCG knows if they are misusing it, or *why* it took MCG three months to reveal little to nothing about the Data Breach.

32. But a breach notice from MCG's customers tells the whole story, which is that MCG knew about the breach as early as December 2021 because cybercriminals had ransomed MCG and posted patient information "for sale" on the dark web:

In December of 2021 and again in January of 2022, MCG was contacted by an unknown third-party who claimed to have improperly obtained patient data from MCG. This third-party made a demand for money in exchange for the return of the patient data to MCG. MCG opened an investigation and contacted the FBI. MCG made Lenoir aware of this incident on April 24, 2022. MCG's forensic investigators confirmed that records for ten (10) patients were listed by this third party for sale on the dark web. These records are believed to have come from MCG. Lenoir patient records were not found on the dark web, but MCG has determined that the unauthorized third-party may be in possession of Lenoir information which could include: patient name, Social Security number, medical codes, street address, telephone number, email address, date of birth and gender.

33. MCG's Breach Notice includes *none* of this information, thus misrepresenting how the breach happened and withholding key information from patients. Indeed, rather than tell patients the truth, MCG downplayed the breach and obfuscated its nature, writing in confusing language that "an unauthorized party previously obtained certain personal information that matched data stored on MCG's systems," without explaining what that means or how it happened.

34. MCG then offered patients two years of credit monitoring and identity theft protection, which does not adequately address the lifelong harm that patients will face following the Data Breach. Indeed, the breach involves PII and PHI that cannot be changed, such as Social Security numbers and birth dates. Further, the breach exposed patients' private health information, a disturbing harm in and of itself.

35. MCG then adds that it has "deployed additional monitoring tools and will continue to enhance the security of our systems"— "tools" and "enhancements" that should have been in place *before* the breach.

36. On information and belief, MCG caused the Data Breach to happen because it failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over patient PII and PHI. MCG's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from

1 accessing PII and PHI. Further, the Breach Notice makes clear that MCG cannot, or will not,
 2 determine the full scope of the Data Breach, as it has been unable to determine exactly what
 3 information was stolen and when.

4 **C. Plaintiffs' Experiences**

5 37. Ms. Crawford is a former patient and employee with an MCG customer,
 6 Newman Regional Health ("Newman").

7 38. Ms. Crawford provided her PII and PHI to MCG through Newman and trusted
 8 that her data would be protected using reasonable means.

9 39. In June 2022, Ms. Crawford received MCG's Breach Notice, establishing that
 10 she is a Data Breach victim.

11 40. Ms. Crawford has and will spend considerable time and effort monitoring her
 12 accounts to protect herself from identity theft. Ms. Crawford fears for her personal financial
 13 security and uncertainty over what PII was exposed in the Data Breach. Ms. Crawford has and
 14 is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the
 15 Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the
 16 sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

17 41. Mr. Price is a former patient with an MCG customer, Indiana University Health
 18 ("IUH").

19 42. Mr. Price provided his PII and PHI to MCG through IUH and trusted that his
 20 data would be protected using reasonable means.

21 43. In June 2022, Mr. Price received MCG's Breach Notice, establishing that he is a
 22 Data Breach victim.

23 44. Mr. Price has and will spend considerable time and effort monitoring his
 24 accounts to protect himself from identity theft. Mr. Price fears for his personal financial
 25 security and uncertainty over what PII was exposed in the Data Breach. Mr. Price has and is
 26 experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the
 27

1 Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the
 2 sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

3 45. Further, following the breach, Mr. Price learned that his son, who is also an IUH
 4 patient, suffered identity theft following the Data Breach.

5 **D. Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity**
 6 **Theft**

7 46. Plaintiffs and members of the proposed Class have suffered injury from the
 8 misuse of their PII and PHI that can be directly traced to Defendant.

9 47. As a result of MCG's failure to prevent the Data Breach, Plaintiffs and the
 10 proposed Class have suffered and will continue to suffer damages, including monetary losses,
 11 lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of
 12 suffering:

- 13 a. The loss of the opportunity to control how their PII and PHI is used;
- 14 b. The diminution in value of their PII and PHI;
- 15 c. The compromise and continuing publication of their PII and PHI;
- 16 d. Out-of-pocket costs associated with the prevention, detection, recovery,
 17 and remediation from identity theft or fraud;
- 18 e. Lost opportunity costs and lost wages associated with the time and effort
 19 expended addressing and attempting to mitigate the actual and future consequences of the Data
 20 Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest,
 21 and recover from identity theft and fraud;
- 22 f. Delay in receipt of tax refund monies;
- 23 g. Unauthorized use of stolen PII and PHI; and
- 24 h. The continued risk to their PII and PHI, which remains in the possession
 25 of defendant and is subject to further breaches so long as defendant fails to undertake the
 26 appropriate measures to protect the PII and PHI in their possession.

1 48. Stolen PII and PHI is one of the most valuable commodities on the criminal
2 information black market. According to Experian, a credit-monitoring service, stolen PII can
3 be worth up to \$1,000.00 depending on the type of information obtained.

4 49. The value of Plaintiffs and the proposed Class's PII and PHI on the black
5 market is considerable. Stolen PII and PHI trades on the black market for years, and criminals
6 frequently post stolen private information openly and directly on various "dark web" internet
7 websites, making the information publicly available, for a substantial fee of course.

8 50. It can take victims years to spot identity or PII and PHI theft, giving criminals
9 plenty of time to use that information for cash.

10 51. One such example of criminals using PII and PHI for profit is the development
11 of "Fullz" packages.

12 52. Cyber-criminals can cross-reference two sources of PII and PHI to marry
13 unregulated data available elsewhere to criminally stolen data with an astonishingly complete
14 scope and degree of accuracy in order to assemble complete dossiers on individuals. These
15 dossiers are known as "Fullz" packages.

16 53. The development of "Fullz" packages means that stolen PII and PHI from the
17 Data Breach can easily be used to link and identify it to Plaintiffs and the proposed Class's
18 phone numbers, email addresses, and other unregulated sources and identifiers. In other words,
19 even if certain information such as emails, phone numbers, or credit card numbers may not be
20 included in the PII and PHI stolen by the cyber-criminals in the Data Breach, criminals can
21 easily create a Fullz package and sell it at a higher price to unscrupulous operators and
22 criminals (such as illegal and scam telemarketers) over and over. That is exactly what is
23 happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of
24 fact, including this Court or a jury, to find that Plaintiffs and other members of the proposed
25 Class's stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data
26 Breach.

54. Defendant disclosed the PII and PHI of Plaintiffs and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII and PHI.

55. Defendant's failure to properly notify Plaintiffs and members of the proposed Class of the Data Breach exacerbated Plaintiffs and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

E. MCG Failed to Adhere to HIPAA

56. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.

57. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is properly maintained.

58. The Data Breach itself resulted from a combination of inadequacies showing SMC failed to comply with safeguards mandated by HIPAA. MCG's security failures include, but are not limited to:

- a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);
- b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

1 c. Failing to protect against any reasonably anticipated uses or disclosures
2 of electronic PHI that are not permitted under the privacy rules regarding individually
3 identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

4 d. Failing to ensure compliance with HIPAA security standards by SMC's
5 workforce in violation of 45 C.F.R. § 164.306(a)(4);

6 e. Failing to implement technical policies and procedures for electronic
7 information systems that maintain electronic PHI to allow access only to those persons or
8 software programs that have been granted access rights in violation of 45 C.F.R. §
9 164.312(a)(1);

10 f. Failing to implement policies and procedures to prevent, detect, contain
11 and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

12 g. Failing to identify and respond to suspected or known security incidents
13 and failing to mitigate, to the extent practicable, harmful effects of security incidents that are
14 known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

15 h. Failing to effectively train all staff members on the policies and
16 procedures with respect to PHI as necessary and appropriate for staff members to carry out
17 their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45
18 C.F.R. § 164.308(a)(5); and

19 i. Failing to design, implement, and enforce policies and procedures
20 establishing physical and administrative safeguards to reasonably safeguard PHI, in
21 compliance with 45 C.F.R. § 164.530(c).

22 **F. MCG Failed to Adhere to FTC Guidelines**

23 59. According to the Federal Trade Commission ("FTC"), the need for data security
24 should be factored into all business decision-making. To that end, the FTC has issued
25 numerous guidelines identifying best data security practices that businesses, such as MCG,
26 should employ to protect against the unlawful exposure of Personal Information.

1 60. In 2016, the FTC updated its publication, Protecting Personal Information: A
2 Guide for Business, which established guidelines for fundamental data security principles and
3 practices for business. The guidelines explain that businesses should:

- 4 a. protect the personal customer information that they keep;
- 5 b. properly dispose of personal information that is no longer needed;
- 6 c. encrypt information stored on computer networks;
- 7 d. understand their network's vulnerabilities; and
- 8 e. implement policies to correct security problems.

9 61. The guidelines also recommend that businesses watch for large amounts of data
10 being transmitted from the system and have a response plan ready in the event of a breach.

11 62. The FTC recommends that companies not maintain PHI longer than is needed
12 for authorization of a transaction; limit access to sensitive data; require complex passwords to
13 be used on networks; use industry-tested methods for security; monitor for suspicious activity
14 on the network; and verify that third-party service providers have implemented reasonable
15 security measures.

16 63. The FTC has brought enforcement actions against businesses for failing to
17 adequately and reasonably protect customer data, treating the failure to employ reasonable and
18 appropriate measures to protect against unauthorized access to confidential consumer data as
19 an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act
20 ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures
21 businesses must take to meet their data security obligations.

22 64. MCG's failure to employ reasonable and appropriate measures to protect
23 against unauthorized access to patient PHI constitutes an unfair act or practice prohibited by
24 Section 5 of the FTCA, 15 U.S.C. § 45.

25

26

27

V. CLASS ACTION ALLEGATIONS

65. Plaintiffs sue on behalf of themselves and the proposed Class (“Class”), defined as follows:

All individuals residing in the United States whose PII and PHI was compromised in the Data Breach disclosed by MCG in March 2022.

Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

66. Plaintiffs reserve the right to amend the class definition.

67. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiffs are representative of the proposed Class, consisting of 1.1 million members, far too many to join in a single action.

b. **Ascertainability**. Class members are readily identifiable from information in Defendant’s possession, custody, and control.

c. **Typicality**. Plaintiffs’ claims are typical of Class member’s claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class’s interests. Their interests do not conflict with Class members’ interests and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class’s behalf, including as lead counsel.

e. **Commonality**. Plaintiffs and the Class’s claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in

1 safeguarding Plaintiffs and the Class's PII and PHI;

2 ii. Whether Defendant failed to implement and maintain reasonable
3 security procedures and practices appropriate to the nature and scope of the information
4 compromised in the Data Breach;

5 iii. Whether Defendant was negligent in maintaining, protecting, and
6 securing PII and PHI;

7 iv. Whether Defendant breached contract promises to safeguard
8 Plaintiffs and the Class's PII and PHI;

9 v. Whether Defendant took reasonable measures to determine the
10 extent of the Data Breach after discovering it;

11 vi. Whether Defendant's Breach Notice was reasonable;

12 vii. Whether the Data Breach caused Plaintiffs and the Class injuries;

13 viii. What the proper damages measure is; and

14 ix. Whether Plaintiffs and the Class are entitled to damages, treble
15 damages, or injunctive relief.

16 68. Further, common questions of law and fact predominate over any individualized
17 questions, and a class action is superior to individual litigation or any other available method to
18 fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs
19 are insufficient to make individual lawsuits economically feasible.

20 **COUNT I**

21 **Negligence**

22 **(On Behalf of Plaintiffs and the Class)**

23 69. Plaintiffs reallege all previous paragraphs as if fully set forth below.

24 70. Plaintiffs and members of the Class entrusted their PII and PHI to Defendant.
25 Defendant owed to Plaintiffs and other members of the Class a duty to exercise reasonable care
26 in handling and using the PII and PHI in its care and custody, including implementing
27 industry-standard security procedures sufficient to reasonably protect the information from the

1 Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at
2 unauthorized access.

3 71. Defendant owed a duty of care to Plaintiffs and members of the Class because it
4 was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with
5 state-of-the-art industry standards concerning data security would result in the compromise of
6 that PII and PHI —just like the Data Breach that ultimately came to pass. Defendant acted with
7 wanton and reckless disregard for the security and confidentiality of Plaintiffs' and members of
8 the Class's PII by disclosing and providing access to this information to third parties and by
9 failing to properly supervise both the way the PII and PHI was stored, used, and exchanged,
10 and those in its employ who were responsible for making that happen.

11 72. Defendant owed to Plaintiffs and members of the Class a duty to notify them
12 within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a
13 duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature,
14 and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and
15 members of the Class to take appropriate measures to protect their PII and PHI, to be vigilant
16 in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm
17 caused by the Data Breach.

18 73. Defendant owed these duties to Plaintiffs and members of the Class because
19 they are members of a well-defined, foreseeable, and probable class of individuals whom
20 Defendant knew or should have known would suffer injury-in-fact from Defendant's
21 inadequate security protocols. Defendant actively sought and obtained Plaintiffs and members
22 of the Class's personal information and PII and PHI.

23 74. The risk that unauthorized persons would attempt to gain access to the PII and
24 PHI and misuse it was foreseeable. Given that Defendant holds vast amounts of PII and PHI, it
25 was inevitable that unauthorized individuals would attempt to access Defendant's databases
26 containing the PII and PHI —whether by malware or otherwise.

76. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII and PHI of Plaintiffs and members of the Class which actually and proximately caused the Data Breach and Plaintiffs and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

76. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII and PHI of Plaintiffs and members of the Class which actually and proximately caused the Data Breach and Plaintiffs and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

77. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII and PHI by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII and PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II

Violation of the Washington Consumer Protection Act, RCW § 19.86, *et seq.*
(On Behalf of the Plaintiffs and the Proposed Class)

78. Plaintiffs incorporate all previous paragraphs as if fully set forth below.

79. Defendant is a “person” under the Washington Consumer Protection Act, RCW § 19.86.101(1), and they conduct “trade” and “commerce” under RCW § 19.86.010(2).

1 80. Plaintiffs and other members of the proposed Class are “persons” under RCW §
2 19.86.010(1).

3 81. Defendant’s failure to safeguard the PII and PHI exposed in the Data Breach
4 constitutes an unfair act that offends public policy.

5 82. Defendant’s failure to safeguard the PII and PHI compromised in the Data
6 Breach caused Plaintiffs and the proposed Class substantial injury. Defendant’s failure is not
7 outweighed by any countervailing benefits to consumers or competitors, and it was not
8 reasonably avoidable by consumers.

9 83. Defendant’s failure to safeguard the PII and PHI disclosed in the Data Breach,
10 and its failure to give time and complete notice of the Data Breach to victims, is unfair because
11 these acts and practices are immoral, unethical, oppressive, and unscrupulous.

12 84. Defendant’s unfair acts or practices occurred in its trade or business and have
13 injured and can injure a substantial portion of the public. Defendant’s general conduct as
14 alleged injures the public interest, and the acts Plaintiffs complain of are ongoing and have a
15 substantial likelihood of being repeated.

16 85. As a direct and proximate result of Defendant’s unfair acts or practices,
17 Plaintiffs and the proposed Class suffered an injury in fact.

18 86. As a result of Defendant’s conduct, Plaintiffs’ and members of the Class’s
19 actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII
20 and PHI by criminals, improper disclosure of their PII and PHI, lost benefit of their bargain,
21 lost value of their PII and PHI, and lost time and money incurred to mitigate and remediate the
22 effects of the Data Breach that resulted from and were caused by Defendant’s conduct, which
23 injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to
24 face.

25 87. Plaintiffs and the proposed Class are entitled to an order enjoining the conduct
26 complained of and ordering Defendant to take remedial measures to prevent similar data
27

breaches; actual damages; treble damages under § 19.86.090; and the costs of bringing this suit, including reasonable attorney fees.

COUNT III

Violation of the Washington Data Breach Disclosure Law (On Behalf of the Plaintiffs and the Proposed Class)

88. Plaintiffs incorporate all previous paragraphs as if fully set forth below.

89. RCW § 19.255.010(2) provides that “[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

90. The Data Breach led to “unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by” Defendant, leading to a “breach of the security of [Defendant’s] systems,” as defined by RCW § 19.255.010.

91. Defendant failed to disclose that the PII and PHI of millions of patients had been compromised “immediately” upon discovery, and in doing so unreasonably delayed informing Plaintiffs and the proposed Class about the Data Breach.

92. A violation under RCW § 19.255 is an unfair or deceptive act in trade or commerce and an unfair method of competition for purposes of applying the consumer protection act under § 19.86.

COUNT IV

Invasion of Privacy (On Behalf of the Plaintiffs and the Class)

93. Plaintiffs incorporate all previous paragraphs as if fully set forth below.

94. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential medical and reproductive histories and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

1 95. Defendant owed a duty to patients, including Plaintiffs and the Class, to keep
2 this information confidential.

3 96. The unauthorized acquisition (*i.e.*, theft) by a third party of Plaintiffs' and the
4 Class's PHI and PII is highly offensive to a reasonable person.

5 97. The intrusion was into a place or thing which was private and entitled to be
6 private. Plaintiffs and the Class disclosed their sensitive and confidential medical information
7 to Defendant's customers as part of their treatment, but did so privately, with the intention that
8 their information would be kept confidential and protected from unauthorized disclosure.
9 Plaintiffs and the Class were reasonable in their belief that such information would be kept
10 private and would not be disclosed without their authorization.

11 98. The Data Breach constitutes an intentional interference with Plaintiffs and the
12 Class's interest in solitude or seclusion, either as to their person or as to their private affairs or
13 concerns, of a kind that would be highly offensive to a reasonable person.

14 99. Defendant acted with a knowing state of mind when it permitted the Data
15 Breach because it knew its information security practices were inadequate.

16 100. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs
17 and the Class in a timely fashion about the Data Breach, thereby materially impairing their
18 mitigation efforts.

19 101. Acting with knowledge, Defendant had notice and knew that its inadequate
20 cybersecurity practices would cause injury to Plaintiffs and the Class.

21 102. As a proximate result of Defendant's acts and omissions, the private and
22 sensitive PHI and PII of Plaintiffs and the Class were stolen by a third party and is now
23 available to disclosure and redisclosure without authorization, causing Plaintiffs and the Class
24 to suffer damages.

25 103. Unless and until enjoined and restrained by order of this Court, Defendant's
26 wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class
27

1 since those medical records are still maintained by Defendant with their inadequate
2 cybersecurity system and policies.

3 104. Plaintiffs and the Class have no adequate remedy at law for the injuries relating
4 to Defendant's continued possession of their sensitive and confidential medical records. A
5 judgment for monetary damages will not end Defendant's inability to safeguard the medical
6 records of Plaintiffs and the Class. In addition to injunctive relief, Plaintiffs, on behalf of
7 themselves and the other members of the Class, also seeks compensatory damages for
8 Defendant's invasion of privacy, which includes the value of the privacy interest invaded by
9 Defendant, the costs of future monitoring of their credit history for identity theft and fraud,
10 plus prejudgment interest, and costs.

11 **COUNT V**
12 **Declaratory Judgment and Injunctive Relief**
(On behalf of Plaintiffs and the Class)

13 105. Plaintiffs incorporate all previous paragraphs as if fully set forth below.

14 106. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is
15 authorized to enter a judgment declaring the rights and legal relations of the parties and to
16 grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such
17 as those alleged herein, which are tortious and which violate the terms of the federal and state
18 statutes described above.

19 107. An actual controversy has arisen in the wake of the Data Breach at issue
20 regarding Defendant's common law and other duties to act reasonably with respect to
21 employing reasonable data security. Plaintiffs allege Defendant's actions in this respect were
22 inadequate and unreasonable and, upon information and belief, remain inadequate and
23 unreasonable. Additionally, Plaintiffs and the Class continue to suffer injury due to the
24 continued and ongoing threat of new or additional fraud against them or on their accounts
25 using the stolen data.
26
27

1 108. Pursuant to its authority under the Declaratory Judgment Act, this Court should
2 enter a judgment declaring, among other things, the following:

3 a. Defendant owed, and continues to owe, a legal duty to employ
4 reasonable data security to secure the PII and PHI with which it is entrusted;

5 b. Defendant breached, and continues to breach, its duty by failing to
6 employ reasonable measures to secure its customers' personal and financial information; and

7 c. Defendant's breach of its legal duty continues to cause harm to Plaintiffs
8 and the Class.

9 109. The Court should also issue corresponding injunctive relief requiring Defendant
10 to employ adequate security protocols consistent with industry standards to protect Plaintiffs
11 and the Class's data.

12 110. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable
13 injury and lack an adequate legal remedy in the event of another breach of Defendant's data
14 systems. If another breach of Defendant's data systems occurs, Plaintiffs and the Class will not
15 have an adequate remedy at law because many of the resulting injuries are not readily
16 quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct.
17 Simply put, monetary damages, while warranted to compensate Plaintiffs and the Class for
18 their out-of-pocket and other damages that are legally quantifiable and provable, do not cover
19 the full extent of injuries suffered by Plaintiffs and the Class, which include monetary damages
20 that are not legally quantifiable or provable.

21 111. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds
22 the hardship to Defendant if an injunction is issued.

23 112. Issuance of the requested injunction will not disserve the public interest. To the
24 contrary, such an injunction would benefit the public by preventing another data breach, thus
25 eliminating the injuries that would result to Plaintiffs, the Class, and the public at large.

VI. PRAYER FOR RELIEF

Plaintiffs and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII and PHI;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

VII. JURY DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 24th day of June, 2022.

TURKE & STRAUSS LLP

By: /s/ Samuel J. Strauss, WBSA #46971

Samuel J. Strauss, WBSA #46971

Email: sam@turkestrauss.com

613 Williamson St., Suite 201

Madison, Wisconsin 53703

Telephone: (608) 237-1775

Facsimile: (608) 509-4423

Attorneys for Plaintiffs